# CYBERSECURITY AND SMART CITIES

**Shalini Kesar**

Southern Utah University (USA)

kesar@suu.edu

## ABSTRACT

This paper outlines some challenges and suggestion to manage and minimize cybersecurity breach within smart cities. It also reviews various research and recommendations proposed to minimize, manage, and mitigate cyber breaches within the smart cities. According to definition, a smart city is designation given to a city that incorporates Information and Communication Technologies (ICT) to enhance the quality and performance of urban services such as energy, transportation and utilities in order to reduce resource consumption, wastage and overall costs. Various reports, worldwide spending on cybersecurity is going to reach $133.7 billion in 2022. Furthermore, smart cities are complex ecosystem where city infrastructure (public and private entities, people, processes, and devices) are constantly interacting with each other and with technology also.

**KEYWORDS:** Smart cities, cyber breaches, ecosystem.

## 1. INTRODUCTION

With increase in technology use, the misuse of it is also on the rise. According to Verizon report (2019): worldwide spending on cybersecurity is going to reach $133.7 billion in 2022; approximately 68% of business leaders feel their cybersecurity risks are increasing; data breaches exposed 4.1 billion records in the first half of 2019; 71% of breaches were financially motivated and 25% were motivated by espionage; and 52% of breaches featured hacking; 28% involved malware; and 32–33% included phishing or social engineering.

Cybersecurity, by definition refers to a set of techniques used to protect the integrity of an organization's security architecture and safeguard its data against attack, damage or unauthorized access. Verizon report (2019) commented that smart cities are increasingly under attack by a variety of threats. Further, "these include sophisticated cyberattacks on critical infrastructure, bringing Industrial Control Systems (ICS) to a grinding halt, abusing Low-Power Wide Area Networks (LPWAN) and device communication hijacking, system lockdown threats caused by ransomware, manipulation of sensor data to cause widespread panic (e.g., disaster detection systems) and siphoning citizen, healthcare, consumer data, and personally identifiable information (PII), among many others," explains Dimitrios Pavlakis, Industry Analyst at ABI Research. "In this increasingly connected technological landscape, every smart city service is as secure as its weakest link." (Help Net Security, 2019).

In general, smart cities use connected technology and data to :1) improve the efficiency of city service delivery; 2) enhance quality of life for all; 3) increase equity and prosperity for residents and businesses. Report by Pandey et al (2019) underlying technology infrastructure of the ecosystem comprises three layers: the edge, the core, and the communication. The edge layer comprises devices such as sensors, actuators, other IoT devices, and smartphones. The core is the technology platform that processes and makes sense of the data flowing from the edge. Whereas the communication layer, establishes a constant, two-way data exchange between the core and the edge to seamlessly integrate the various components of the ecosystem. Consequently, with the growth of smart cities that is projected to increase fourfold by 2025, cybercrime will also continue to rise within smart cities.

## 2. CYBER CRIME IS ON THE RISE

Across the globe, cybersecurity breaches are increasing. Recent report conducted by Symantec Internet Security Threat Report (2019) highlighted some alarming figures: an average of 4,800 websites compromised each month; Ransomware shifted targets from consumers to enterprises, where infections rose 12 percent; More than 70 million records stolen from poorly configured S3 buckets, a casualty of rapid cloud adoption; Internet of Things (IoT) was a key entry point for targeted attacks. In addition to the statistics above, Verizon Report (2019), states that the most common causes of data breach include: weak and stolen credentials; passwords; Back Doors; Application Vulnerabilities; Malware; Social Engineering; Too Many Permissions; Insider Threats; Improper Configuration; and User Error.

### 2.1. Smart cities and technology

Smart cities are the future, especially in urban area to boost the efficiency and effectiveness of city services. Amsterdam was one of the first European cities to launch a smart city program, with the goal of improving its economy, environment, government, living, and mobility. Some of their qualifications for becoming a smart city are: smart housing; open data; smart grids; home energy storage; connectivity; and smart mobility. Currently, only 600 urban cities contribute to 60% of global GDP. The idea of a smart city is to collect information through connected devices and make life more comfortable using these devices for logistics. It is estimated that the market for smart city technology is expected to reach $1.5 trillion by 2020. One smart city initiative is Singapore’s “Smart Nation” project, that aims to apply new technologies to enhance transportation systems, health, home and business. (Sivaramakrishnan, 2017). The goal is to increase interconnectedness in all aspects of citizens’ lives through digital technologies. The underlying goal for Singapore smart city is: healthier citizens mean healthier cities; a house with a heart is a home; and mobility is a shared community experience. China, is another example, where it aims to develop 103 smart cities. These smart cities seek to bring pollution, traffic congestion and widespread energy consumption under control through greater use of connected technologies. Within India, 90 cities are targeted to develop smart capabilities as part of its “Smart City Mission.” Their pragmatic approach is to attack this initiative in a layered approach, solving specific issues one at a time. Since 2011, Tokyo (Japan) has focused heavily on becoming greener by integrating homes with solar panels as well as attaching those homes to a smart grid. Policies are being modified to integrate a more sustainable and an eco-friendly infrastructure. Within the United States, cities such Boston, Las Vegas, Kansas City, and Chicago are all taking advantage of smart solutions to address transportation, sanitation, connectivity, and safety issues in their communities. Other cities within the United States include, Columbus, Pittsburgh, Denver, San Francisco, and Dallas (Condliffe, 2016). They are implementing smart technology in innovative ways to incorporate transportation as part of the smart city strategy to better connect citizens to human services; encourage greater use of sustainable transportation; improve access to jobs; and provide real-time traffic information to improve commuter mobility. Investments for some cities include in millions of US dollars.

One of the consequences of building a smart city is systems, sensors and devices are not only connected to each other and to external systems around the world but also are increasingly connected with over lightning-fast networks via the public internet and a wide range of cloud computing architectures. The more things that are connected, the greater the opportunity for cyber breaches to infiltrate your systems, exfiltrate sensitive data and disrupt potentially critical systems used in law enforcement, public health and other municipal applications.

### 2.2. Smart cities and cyber breaches

As mentioned above, this new wave of digital transformation also brings new cyber risks that could fundamentally impact the existence of smart cities. Cyber threats have been on the rise for years, but the last few years have seen an explosion in cyberattacks that target both data and physical assets. No doubt citizens benefit from living in smart cities. However, at the same time technology brings risks and vulnerabilities to cybersecurity. There are many examples of cyber breaches in smart cities that have warrant us to think about the consequences and solutions. For example, Atlanta, capital of Georgia State in the United States, faced SamSam, a ruthless “ransomware” bug in March 2019. This lasted approximately two weeks and a cost $55,000 worth of bitcoin in payment was demanded. The aftermath of denying the demand left Atlanta City processing reports and legal documents, which cost of this attack in millions. Baltimore, another smart city in the United States faced cyber breach. The attack involved a ransomware attack that led to accessibility issues to their Computer Aided Dispatch (CAD) system of Emergency services for 17 hours. The city’s Emergency services relied on this system to automatically divert calls to emergency responders who are closest in location so that emergency assistance is directed as efficiently as possible. While the system was down responders operated by taking phone calls manually, a far slower process that could have had a more sinister outcome if the cyber-attack had been prolonged. There are many other examples of cyber breaches in smart cities. Another example, San Francisco Municipal Transportation Agency example when hackers used ransomware to shut down its ticketing systems and demand payment (Condliffe, 2016).

It has been pointed out that by 2050, about 66% of the world’s population is expected to live in cities. Methods to minimize, manage, and mitigate cyber breaches should be one of the first priority while using advanced technologies within smart cities. While developing solutions, it is important to keep in mind some of the realities of cybersecurity in smart cities, for example: 1) The introduction of new web and mobile apps, IoT, connected homes, connected cars and even connected logistics. The increase use of such new technologies will make more data and gadget accessible to criminals; 2) Cybercriminal motivations increase to get access to IoT. The sophistication of technology also means increases in skills and tactics of cyber criminals; 3) Lack of skill of cybersecurity experts. Statistics indicate there is more demand than supply for cybersecurity experts. This reality can become a problem as cities become more dependent on technology for everyday activities. In addition to the realities of cybersecurity and smart cities, ethical implications also become a concern. The U.S. Department of Transportation issued a “Smart City Challenge,” to U.S. cities, encouraging them with funding to develop more smart technologies around transportation. The hope is that, as cities compete, they will develop ways to use digital technology to solve transportation problems and improve efficiencies. As ideas are developed, other cities can then adapt them to their needs.

## 3. THREE LAYERS OF ECOSYSTEM AND CYBER CRIME

To help address some of the challenges mentioned above, researchers have argued that cities should embed cybersecurity principles to minimize, manage, and mitigate cyber breaches. This paper uses the framework proposed in the article “Making smart cities cybersecure Ways to address distinct risks in an increasingly connected urban future”, by Pandey et al (2019). They outline three layers of ecosystem in context of smart cities: the edge, the core, and the communication. This paper also reviews cybersecurity challenges in the ecosystem of smart cities. According to Pandey et al, there are three factors influence the potential cyber risk in a smart city ecosystem: Convergence of the cyber and physical worlds; Interoperability between legacy and new systems; and Integration of disparate city services and enabling infrastructure.

This section reviews the challenges and reflects on the three layers of the ecosystem and cyber risks in context of smart cities. This is significant since it is estimated that the world’s urban population will rise by 72 per cent between 2011 and 2050. To combat this growing demand, it is important to keep a check on use and misuse of technology, especially within smart cities. Furthermore, it becomes critical that smart cities service providers such as networking Internet of Things (IoT) technology with existing infrastructure are balanced and reshape supply chains and manage assets and resources more efficiently.

### 3.1. The core layer

This layer deals with technology platform, such as cloud, Internet of Things (IoT), that process data. This layer also enables to generate business logic to make sense of data following from the edge layer. As mentioned above, more than half of globe is spending money to connect cities with technologies to provide resilient energy infrastructure, data-driven public safety or intelligent transportation. Examples above describe cities from San Francisco’s smart power grid to Barcelona’s digitized waste management systems. With the smart cites projects come unintended consequences to all those infrastructures connected with technologies. It is true to state that the more things that are connected, the greater the opportunity for cyber attackers to infiltrate such systems, exfiltrate sensitive data and disrupt potentially critical systems used in law enforcement, public health and other municipal applications.

Moving towards smart city strategy requires careful consideration of reviewing polices. Examples of cyber breach cases in smart cities of Atlanta, Baltimore and Sint Martens, recent report by DiliTrust (2019) criticized by development experts as having been “procured and developed with little coordinated consideration of privacy and security harms”.

Accurate recovery from a cyber-attack depends on fast and perfect damage assessment. According to Anderson (2019), cyberattacks, regulators that are beginning to introduce expansive rules for tech usage and data protection should be in close proximity as part of response of relentless data breaches. In addition, at the core layer, cities should define a detailed cybersecurity strategy that is in line with their broader smart city strategy to mitigate challenges arising from the ongoing convergence, interoperability, and interconnectedness of city systems and processes. Risk management assessments that identify assets, vulnerabilities and threats will help organizations manage, minimize, and mitigate breaches associated with technology adoption. The integrated view of the risks and knowledge of interdependencies of the critical assets can enable cities to develop a comprehensive cybersecurity strategy. In the Catapult Future Cities report (2017), various strategies were discussed with examples of different countries. The report suggested smart city strategies are made through collaborative stakeholder engagement with city stakeholders and citizens. It is critical that they follow an approach that is well-understood with the existing breaches and have a buy-in with the stakeholders that need to deliver it. There is no doubt that such an approach will takes longer to complete and implement smart cities core infrastructure. Some of the recommendation proposed in the article can be applied to any smart city context. For example, establish strong leadership to develop skills and capacity within local government to deliver at-scale smart city projects (Catapult Future Cities, 2017).

A great example, is Tel Aviv smart city. They have included champions and training their council staff as part of their smart city core strategy. Core city plans that include smart city strategy within existing statutory frameworks can also prove to be a beneficial and smooth transition process. Sydney and São Paulo ae two examples that have embedded their city plans when creating their smart city strategy. Modification or revising polices linked with existing cyber security laws and acts is part of the core when creating policies. For instance, Singapore launched its National Cyber Security Master plan in 2013 and followed it with a new cyber security bill in 2016. Both initiatives were an integral part of Singapore's smart nation strategy. This is because with use of technology, the misuse of technology also increases.

### 3.2. The communication layer

Communication layer is related to the technology gadgets like Bluetooth and wireless. Different cities have utilized different mechanism to build a smart infrastructure. The Songdo International Business District, as it's formally known, was built from scratch, on reclaimed land from the Yellow Sea. It has the state of art communication layer to support the 1,500-acre development of smart city. New Songdo City was envisioned as "a giant test bed for new technologies' that would demonstrate the country's technological prowess to help attract foreign investment" (Poon, 2018). Programs like these aim at using technology gadgets to improve life in cities, whilst attracting foreign investment to increase economic growth.

Innovations in the communication layer of smart cities are also increasing the risks of cyber breaches and data comprise. As highlighted above, statistics highlight the increases of cyber breaches. Hence it is true to say that such cities thriving to become smart will require to explore new techniques and policies to solve cyber-related issues. Managing, minimizing and mitigation cyber breaches within smart cities requires attention from strategy and design to implementation and operations. Elmaghraby et al (2014), in their article "Cyber Security Challenges in Smart Cities: Safety, security and privacy", suggest a framework linked with privacy solutions and smart cities.

### 3.3. The edge layer

The edge layer comprises of sensors, actuators, and smart phones. This is the front end of the smart cities. A classic example of comprise of the edge layer is the 2018 case when Emotet malware virus struck the city of Allentown, Pennsylvania. The virus quickly multiplied in a week and rendered the city's finance department system unusable by not allowing it to make external bank transactions. Also, the police department could not access databases controlled by the Pennsylvania state police. Containing the virus and getting back to operational status is estimated to have cost the city US$1 million. Some of the vulnerabilities of the smart systems can be the traffic control systems. Cases have highlighted how smart traffic control systems are vulnerable to takeover. The 2006 case of a disgruntled employees who attacked Los Angeles traffic control systems is another example of communication layer being compromised. Although an increasing number of newer smart systems have the necessary state of art technologies, however older systems currently installed lack it and would be very hard to replace without major street reconstruction. Attacks on traffic and surveillance cameras, too, could render a city blind. The 2016, ransomware attack on the San Francisco municipal rail system demonstrates that municipal transit systems are being targeted. Additionally, introducing false information on the systems could comprise privacy of citizens. Other cases of cyber breaches include, 2015 BlackEnergy attack on the Ukrainian power grid, where more than 80,000 consumers were left without power. Another case is the 2016 hack of an unidentified water treatment plant, where mass casualties were averted only because the hacktivists who attacked it did not immediately realize what toxic chemicals they were in a position to unleash on the plant's consumers (See Verizon report 2019 for details for the cases).

When it comes to smart cities, privacy concern is a topic that comes to the forefront. According to AlDairi and Tawalbeh (2017), smart cities influencers must pay more attention so security and privacy concerns in smart cities. In their paper, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies', they discuss major security problems and recommendations linked with current smart cites. Further, they present several influencing factors that can affect data and information security in smart cities. They outline five main components that are essentially required to be in a smart city: modern information and communication technologies, buildings, utilities and infrastructure, transportation and traffic management and the city itself.

## 4. CONCLUSION

In addition to advantages of smart cities, the tremendous data exchange and integration of technologies within the three layers of the ecosystem can create higher cyber risks and threats. The dynamically changing of innovative technologies can also result in complexities that requires attention before we play catch up. In context of cyber security, smart cities should into account the three layers of the ecosystem to manage, minimize or mitigate various challenges that could be posed due to the interconnectivity of technology that makes a city smart.

## REFERENCES

Anderson, B. (2018), How to Improve Cybersecurity in a Smart City. *ReadWrite.* Retrieved from https://readwrite.com/2018/11/12/how-to-improve-cybersecurity-in-a-smart-city/

AlDairi, Anwaar, Tawalbeh, Lo'ai. "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies", *8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology*, SEIT 2017, 16-19.

Condliffe, Jamie (2016). Ransomware Took San Francisco's Public Transit for a Ride. *MIT Review*. Retrieved from https://www.technologyreview.com/2016/11/28/69496/ransomware-took-san-franciscos-public-transit-for-a-ride/

DiliTrust (2019), Cyber Attacks on Smart Cities: Why we Need to be Prepared. Retrieved from https://www.dilitrust.com/en/blog/cyber-attacks-smart-cities/

Elmaghraby, Adel & Losavio, Michael (2014). Cyber Security Challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research.* 5(10).1016/j.jare.2014.02.006.

Catapult Future Cities (2017). Smart City Strategies: A Global review. Retrieved from https://futurecities.catapult.org.uk/press-release/first-global-review-smart-cities-published/

Help Net Security (2019). Cybersecurity challenges for smart cities: Key issues and top threats. Retrieved from https://www.helpnetsecurity.com/2019/08/21/cybersecurity-smart-cities/

Pandey, Piyush., Golden, Deborah., Peasley, Sean., & Kelkar, Mahesh (2019). Making smart cities cybersecure: Ways to address distinct risks in an increasingly connected urban future . *Deloitte*

*Insights*. Retrieved from https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html.

Poon, Linda (2018). Sleepy in Songdo, Korea's Smartest City. *City Lab*. Retrieved from https://www.citylab.com/life/2018/06/sleepy-in-songdo-koreas-smartest-city/561374/

Sivaramakrishnan, Sharmishta (2019). 3 reasons why Singapore is the smartest city in the world Retrieved from https://www.weforum.org/agenda/2019/11/singapore-smart-city/

Symantec Security (2019). Internet Security Report. Retrieved from https://www.frontiersin.org/articles/438810

Verizon (2019). 2019 Data Breach Investigations. https://enterprise.verizon.com/en-gb/resources/reports/dbir/